2009/2010 : Report 10

OFFICE OF THE

Auditor General of British Columbia

Wireless Networking Security in Government:

Phase 2

March 2010

2009/2010 : Report 10

OFFICE OF THE

Auditor General of British Columbia

Wireless Networking Security in Government:

Phase 2

March 2010

Library and Archives Canada Cataloguing in Publication Data

British Columbia. Office of the Auditor General.

Wireless networking security in government : phase 2.

(Report ; 2009/2010: 10)
Includes index.
Includes bibliographical references.
ISBN 978-0-7726-6263-7

1. Administrative agencies--Computer networks--Security measures--British Columbia--Evaluation. 2. Wireless communication systems--Security measures--British Columbia. 3. Government communication systems--Security measures--British Columbia. 4. Wireless communication systems--Security measures. 5. Computer security. I. Title. II. Series: British Columbia. Office of the Auditor General. Report ; 2009/2010 : 10.

QA76.9.A25 B76 2010 352.3'79 C2010-901299-2

OFFICE OF THE
Auditor General
of British Columbia

LOCATION:
8 Bastion Square
Victoria, British Columbia
V8V 1X4

OFFICE HOURS:
Monday to Friday
8:30 a.m. – 4:30 p.m.

TELEPHONE:
250 387-6803
Toll free through Enquiry BC at: 1 800 663-7867
In Vancouver dial: 604 660-2421

FAX: 250 387-1230

E-MAIL: bcauditor@bcauditor.com

WEBSITE:
This report and others are available at our website, which also contains further information about the Office: www.bcauditor.com

OFFICE OF THE
Auditor General
of British Columbia

8 Bastion Square
Victoria, British Columbia
Canada V8V 1X4
Telephone: 250 387-6803
Facsimile: 250 387-1230
Website: www.bcauditor.com

The Honourable Bill Barisoff
Speaker of the Legislative Assembly
Province of British Columbia
Parliament Buildings
Victoria, British Columbia
V8V 1X4

Dear Sir:

I have the honour to transmit herewith to the Legislative Assembly of British Columbia my 2009/2010 Report 10: Wireless Networking Security in Government: Phase 2.

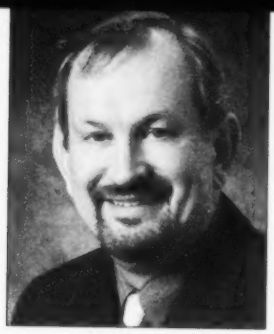
John Doyle, MBA, CA
Auditor General of British Columbia

Victoria, British Columbia
March 2010

copy: Mr. E. George MacMinn, Q.C.
Clerk of the Legislative Assembly

Table of Contents

Auditor General's Comments



John Doyle
Auditor General

Without a doubt, the main advantage of wireless technology is its flexibility. Wireless technology enables organizations to extend their corporate network and maximize user movement within offices—and to do so much more quickly, efficiently and often more cheaply than wired technologies allow. In many businesses, the ability to roam the premises while remaining connected to the Internet and other network resources has become essential to productivity. At educational institutions, such ease of access is now considered imperative.

But wireless computing and its significant benefits come with equally significant risks. Transmissions from wireless devices can be picked up by anyone using the right equipment within range. This makes the risk of broadcast information being received and read by unintended recipients very high. An organization may be under surveillance yet never know it, at least not unless a breach is realized.

New and stronger data encryption methods are being developed to protect wireless data transmissions, but so are new methods of breaking these encryption systems. For instance, computer scientists recently developed the means to quickly break the common wireless encryption WPA. Up until then, WPA had been considered acceptable security for most wireless network communication.

It is this ever-changing environment that makes it vital for organizations to regularly review the vulnerabilities of their wireless networks; to develop rigorous security policies, procedures and standards; and to vigilantly monitor all network activities.

In my first audit report on wireless network security, published in February 2009, I pointed out serious gaps in government wireless networking at locations in Greater Victoria. I also indicated that my Office planned to build on that initial work, expanding audit coverage into other areas of government (including Crown agencies and SUCH sector entities: schools, universities, colleges and health authorities) and investigating other aspects of wireless computing security, such as unauthorized wireless access points.

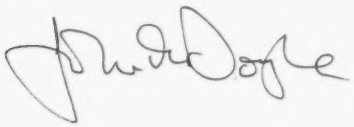
For this second audit, we selected five ministries and two post-secondary educational institutes—Simon Fraser University (SFU) and British Columbia Institute of Technology (BCIT)—in which to conduct a detailed review of wireless networking security. As well, we examined the adoption of policies and procedures and the

supervision of wireless networking activities. This work also gave us the opportunity to find out how much progress government made in addressing the vulnerabilities we identified in our first audit.

Overall, we found that government had made some progress in securing its wireless networking environment. However, greater effort is still needed to ensure ministries comply with the policies and procedures that safeguard wireless transmissions. And while SFU and BCIT demonstrated adequate security settings for their wireless network infrastructures, we concluded that their management and monitoring efforts left room for improvement.

I plan to continue to extend my review of wireless network security to other ministry offices, Crown agencies and SUCH sector entities on a rotational basis as part of my annual financial audit plan. As part of this, I will also examine the security of other wireless computing devices, such as personal digital assistants.

I would like to thank the staff of the selected ministries and the Office of the Chief Information Officer, BCIT and SFU for the cooperation and assistance they provided my staff during their work on this audit.



John Doyle, MBA, CA
Auditor General of British Columbia

Victoria, British Columbia
March 2010

Audit Team

Bill Gilhooly, Assistant Auditor General

David Lau, IT Audit Director

Raveendran Madappattu, IT Audit Manager

Executive Summary

In British Columbia, as everywhere around the world, wireless technologies—such as laptop computers, cell phones and Blackberries—are being rapidly and widely adopted by government offices, Crown entities and post-secondary institutions. While such technologies are flexible and economical to implement, they are also inherently more difficult to secure than wired networks are. "Listening in" to the transmission of confidential information is possible for anyone—accidentally or intentionally—if he or she has the right equipment and is sitting in the right spot to receive data over poorly secured and poorly encrypted wireless networks.

We issued a report on the subject, *Wireless Networking Security in Victoria Government Offices*, in February 2009. Although the scope of the audit on which that report was based was limited to external scanning of government offices, we found significant deficiencies and gaps in how wireless networks in many provincial government buildings were being secured. The government accepted our recommendations and has since taken steps to correct many of the deficiencies we identified.

Between July and September 2009, we did a follow-up audit. This time we expanded the depth of our review to examine policies and procedures adopted by government for managing and securing its wireless networks and for monitoring wireless networking activities. We also expanded our sample size by looking at offices across the province in five government ministries and at campuses of two large provincial post-secondary institutions; Simon Fraser University (SFU) and the British Columbia Institute of Technology (BCIT).

Our findings showed that although the government had addressed many of our previous security concerns, it still fell short in its monitoring efforts to ensure that only authorized and properly configured wireless devices are connected to ministry networks. As well, we found that both SFU and BCIT need to improve security measures such as strengthening their policies and standards for wireless networking, managing and monitoring of wireless operating activities, and better separating roles and responsibilities within their IT departments.

We issued, and cleared, detailed management reports of our findings and recommendations with the senior IT management of each entity we audited. In this report, we summarize only

our high-level key findings—not the details—in the interests of protecting public sector wireless networks from potential accessibility by unscrupulous users.

Given that wireless technology is now an integral part of the corporate IT network, we believe that the review of wireless security should be part of our annual audit on IT general controls. We are therefore considering adding to our future financial audits, on a rotational basis, a review of wireless security in the province's other government offices, Crown entities and educational institutions.

Overall Conclusion

Government

Since our last audit, the government has adopted more comprehensive policies, standards and procedures for ensuring it maintains a secured wireless infrastructure.

The security around government's wireless infrastructure is generally adequate, but the process of monitoring wireless networking activities must be strengthened to ensure ministries are in compliance with policies and procedures to safeguard wireless transmissions.

Simon Fraser University (SFU)

Simon Fraser University's wireless network security is generally adequate, but improvements are needed in areas such as: enhancing policies and standards in wireless networking; strengthening the governance structure of its IT division, the management and monitoring of wireless operating activities, as well as the role and responsibilities of staff who are charged with the responsibilities of overseeing IT security.

British Columbia Institute of Technology (BCIT)

Wireless network security at BCIT is also generally adequate, but improvements are needed in areas such as: enhancing policies and standards in wireless networking, strengthening some of the management and monitoring of wireless operating activities, as well as clearly defining the roles and responsibilities of staff within the IT division.

Wireless Security Audit: Summary of Criteria Assessed and Overall Results

 Not achieved

 Substantially achieved

 Fully achieved

Criterion	Government	Simon Fraser University (SFU)	British Columbia Institute of Technology (BCIT)
A. Maintain effective management of wireless security			
a) Establish and maintain adequate policies, procedures, guidelines and standards for wireless local area networks (WLANs)			
b) Assign responsibility for wireless security			
c) Maintain documentation of wireless architecture			
d) Formally approve wireless technology deployment			
e) Maintain a current list of wireless approvals			
f) Use secure methods to administer wireless devices			
B. Secure wireless infrastructure			
a) Securely configure wireless devices			
b) Deploy updates and security patches			
c) Encrypt wireless traffic			
d) Implement physical security controls to limit unauthorized wireless activity			
C. Monitor wireless security			
a) Maintain an inventory of wireless devices on the network			
b) Monitor wireless activity logs			
c) Monitor for unauthorized wireless activities			

Summary of Recommendations

The number of detailed recommendations we made for each area we assessed is shown below.

Key audit area	Government	Simon Fraser University (SFU)	British Columbia Institute of Technology (BCIT)
A. Maintain effective management of wireless security	3	6	3
B. Secure wireless infrastructure	–	–	–
C. Monitor wireless security	2	2	1
Total recommendations	**5**	**8**	**4**

Government

A. Maintain effective management of wireless security

We recommend that, to support the government's IM/IT (information technology and management) policies relating to wireless network security, the government establishes adequate procedures to ensure ministry compliance with the policies as established by the Office of the Chief Information Officer.

We recommend that Shared Services BC regularly update the job descriptions of all key IT personnel to ensure the roles and responsibilities are clearly delineated.

We recommend that the government develop a network access control solution for monitoring and detecting, on a real time basis, unauthorized computing devices—particularly wireless—connected to the government network, including devices that are not configured properly.

B. Secure wireless infrastructure

No recommendations.

C. Monitor wireless security

We recommend that Shared Services BC implement mechanisms and procedures to scan and confirm that only properly configured and authorized wireless access devices are installed when connecting to the government network infrastructure.

We recommend that for monitoring purposes, Shared Services BC develop a process for establishing and updating an inventory list of authorized wireless access devices and that the list be verified periodically.

Simon Fraser University (SFU)

A. Maintain effective management of wireless security

We recommend that SFU:

- establish a formal IT committee with a strong mandate to oversee IT strategic direction, IT needs of the university community and, most importantly, the protection of the university's IT network;
- establish an IT Security Officer position that has exclusive duties and responsibilities relating to IT security and is accountable to independent senior management;
- ensure that the Information Security Policy is supported with detailed wireless security standards and procedures to guide the implementation and maintenance of a robust wireless security network;
- establish policy and procedures to ensure that users are formally and regularly asked online to accept the policy for appropriate use of communication technology (including wireless) provided by the university;
- enforce periodic change of password; and
- require staff with high-level access rights to systems, applications and data to access system resources using secured wireless methods only.

B. Secure wireless infrastructure

No recommendations.

C. Monitor wireless security

We recommend that SFU:

- conduct review to limit the use of ad hoc and peer-to-peer networking; and
- while monitoring wireless networking activities, ensure that log reviews are fully documented and include such information as the type of reports reviewed, the date of the review, and what action has taken place.

British Columbia Institute of Technology (BCIT)

A. Maintain effective management of wireless security

We recommend that BCIT ensure its policies address wireless network infrastructure in detail, and that the policies be supported by detailed wireless networking standards and specific procedures and guidelines for managing wireless network resources.

We recommend that BCIT's management review its policies to ensure that those relating to ad hoc and peer-to-peer networking, the enforcement of password security, and retention of activity logs generated by wireless systems follow recognized best practices.

We recommend that management require, in policy, staff with higher level access rights to systems, applications and data to log on using secured wireless methods only.

B. Secure wireless infrastructure

No recommendations.

C. Monitor wireless security

We recommend that job positions in IT network operations be supported by clearly defined responsibilities to ensure incompatible duties are not assigned to one individual. If segregation of duties is not possible or feasible because of resourcing limitations, we recommend that there be closer management oversight of the activities carried out by those in IT network operations.

Government — from the Ministry of Citizens' Services

The Ministry of Citizens' Services supports and appreciates the ongoing efforts of the Office of the Auditor General in auditing wireless network security. The Government of British Columbia places a high priority on the protection of information. The wireless security audit has provided valuable information that will contribute to our ongoing efforts to protect information and technology resources, as well as to provide important information security policies, standards and awareness opportunities.

The Government of British Columbia has established information security policies and relevant standards to address potential security threats and risks. To address wireless security risks, the Office of the Chief Information Officer developed and published wireless security standards and the cryptographic standards in February 2009.

To improve the level of policy and standards compliance, the Office of the Chief Information Officer is developing an information security audit program and improving security awareness across government. Shared Services BC is developing an enhanced and cost-effective network access control mechanism to facilitate the implementation of technical countermeasures against wireless security risks.

The Ministry of Citizens' Services appreciates the recommendations provided by the Auditor General. The recommendations will assist in the continuous improvement of the government's wireless network security.

Kim Henderson
Deputy Minister

Responses to the Report

Simon Fraser University (SFU)

Stronger IT Governance

The CIO has prepared a proposal for an IT governance framework for SFU, and the proposal has received initial approval at the senior management committee consisting of the president and vice-presidents. It will be considered shortly by the extended committee that also includes all the deans. Assuming the proposal is approved in essentially its current form, it will augment the current project-management committees with one for the strategic use of IT across the university, one each for the strategic use of IT in research, administration, and teaching & learning, and an operations committee tasked with routine supervision of the large portfolio of ongoing administrative IT projects.

Once the new committees are operational, policies and procedures related to IT, and to wireless security in particular, will be drafted and forwarded through the committees to the appropriate university-level bodies (if required). This will include an examination of policies and procedures for soliciting acceptance of policies for acceptable use of IT resources.

In parallel, IT Services will provide documentation on suggested wireless security standards and procedures.

Separation of Duties

A single employee managed by a senior executive is not a feasible management model in the SFU environment. Staff in ITS with responsibility for security including wireless will continue to be managed as they are today. However, the senior security staff member will have formal access to the university's Internal Auditor, including monthly meetings between the two of them.

Management and Monitoring of Wireless

We will continue to monitor wireless activity on campus with available resources. Given a university environment where experimentation and innovation are encouraged, and where most network devices (belonging to students) are unmanaged by the university, a small amount of ad hoc and peer-to-peer networking

is expected (although not desired). Policy in this regard will become the responsibility of the new governance structure.

Periodic password changes have been discussed at length at all levels at SFU, and there is a general split in the entire industry about whether the ways people find to "remember" their changing passwords are better or worse than an unchanging password. Most recently at SFU at its meeting of December 1, 2009, the Board Audit Committee agreed with management's response to the 2009 Management Letter Recommendations: "There are different professional opinions on whether frequent password changes are beneficial or detrimental to security. Our opinion is that frequent changes would have a detrimental impact."

We will review our use of the insecure SSID "SFUNET", and will consider terminating it. Should that not prove feasible, we will develop policy to require staff and students to use "SFUNET-SECURE" or "eduroam" to access SFU network resources in a secure fashion.

Monitoring Wireless Activities

While more audit reports of log reviews could certainly be assembled, this does not appear to add significant value to our wireless security, particularly in view of the automatic monitoring for certain types of unauthorized use that is performed currently by our Enterasys Dragon Security Command Console.

J. P. Black
Chief Information Officer

British Columbia Institute of Technology (BCIT)

Recommendation 1:

We recommend that the IT Policies of BCIT be extended to include detail on the wireless network infrastructure, and that the policies be supported by adequate detailed and specific procedures and/or guidelines to manage wireless network resources.

Response: We agree with this recommendation. BCIT's policies are based on an international standard (ISO 1799:2005), and are intended to be independent of the network technology. Information specific to the security requirements and characteristics of each network zone is intended to be included in the "Procedures and Guidelines" associated with the policy. According to section "5.6 - Network Management" of Policy 3502 (Information Security Policy) last updated January 2009, each network zone, including the wireless zones, should have "....documentation covering its topology, configuration, and gateways to external networks and nodes...." and "...clear guidelines and...security characteristics". These are being documented as part of the "procedures and guidelines" associated with this policy, and are expected to be complete by June 2010.

Recommendation 2:

We recommend management review their policies to ensure those relating to:

- ***ad hoc and/or peer-to-peer networking,***
- ***enforcement of password security, and***
- ***retention of activity logs generated by wireless systems follow recognized best practices.***

Response: We agree with this recommendation. All BCIT policies have a regular and predictive review schedule. BCIT's Information Security policy (Policy 3502) expressly addresses access control and password use requirements, as well as logging requirements for user activities. Specific details are being documented as part of the "procedures and guidelines" associated with this policy, and are expected to be complete by June 2010.

Recommendation 3:

We recommend that management review the policies to ensure that staff with higher level access rights to systems, applications and data should be required to access systems using secured wireless methods only.

Response: We agree with this recommendation. BCIT's priority however is to ensure end-to-end encryption. This ensures full protection and security regardless of where the user is accessing the application/data. As users are becoming more mobile and accessing systems remotely using network segments that are beyond the control of BCIT/ITS (for example, hot spots in airports, cafes, business centres in hotels, etc.), applying end-to-end level security and encryption will ensure that data is consistently protected regardless of where the user is accessing it. Additionally, BCIT has now implemented a secure VPN gateway for accessing data and systems from off campus. We will continue to promote the use of the secured Eduroam network for administrative users accessing applications and data wirelessly on campus, and will ensure that all "administrative" users accessing the wireless network on campus will be using Eduroam by default within 2 years.

Recommendation 4:

We recommend that job positions be supported by clearly defined responsibilities in IT network operations to ensure incompatible duties are not assigned to one individual. If the segregation of duties in not possible or not feasible due to resourcing limitation, we recommend a closer management oversight of the activities that were carried out by those individuals.

Response: Policy 3501 (Acceptable Use of Information Technology) expressly states that "IT Administrators and other privileged users must protect the security of information and must not abuse their elevated privileges". BCIT IT Services operates under the ITIL framework and best practices for Change Control. This requires any system level change (software, infrastructure, etc.) be planned, reviewed, and approved by the Change Advisory Board (CAB) that has both Management and departmental technical resources allocated to this activity.

The CAB has the authority to approve or deny any updates, changes, additions to the IT environment.

Will Hopkins
Director, IT Services

Detailed Report

Background

Wireless technologies enable one or more electronic hardware devices to communicate without being physically connected. Whereas *wired* technologies use cables to transmit data, *wireless* technologies use radio frequencies for transmission. The latter technologies range from complex systems such as wireless local area networks (WLANs), cell phones and personal digital assistants (for example, Blackberries) to simple devices such as wireless headphones, microphones and other devices that do not process or store information.

In the last decade, significant technological advances have increased the speed and reliability of wireless technologies, resulting in broad, mainstream acceptance and use of them across society.

Wireless computing has become widely adopted in government, business and academic settings

Wireless networks use radio waves to transmit data to wireless-enabled devices such as laptops and personal digital assistants. Access is provided by small base stations, also called access points, installed throughout a "Wi-Fi" environment. These stations can exchange signals with enabled devices that are within range—generally up to 100 metres.

Wireless computing connection points are widely available in many public places. A user can sit in any "hotspot"—such as a hotel, shopping centre, coffee shop, library, school, airport or business—and connect untethered to a host computer, network or online service provider. This ease of access is the result both of the new wireless communication standards and methods that significantly increase wireless bandwidth (the data transmission rates), and of the decreasing costs of equipment such as laptops and connectivity devices. Wireless connections are also relatively simple to install and use.

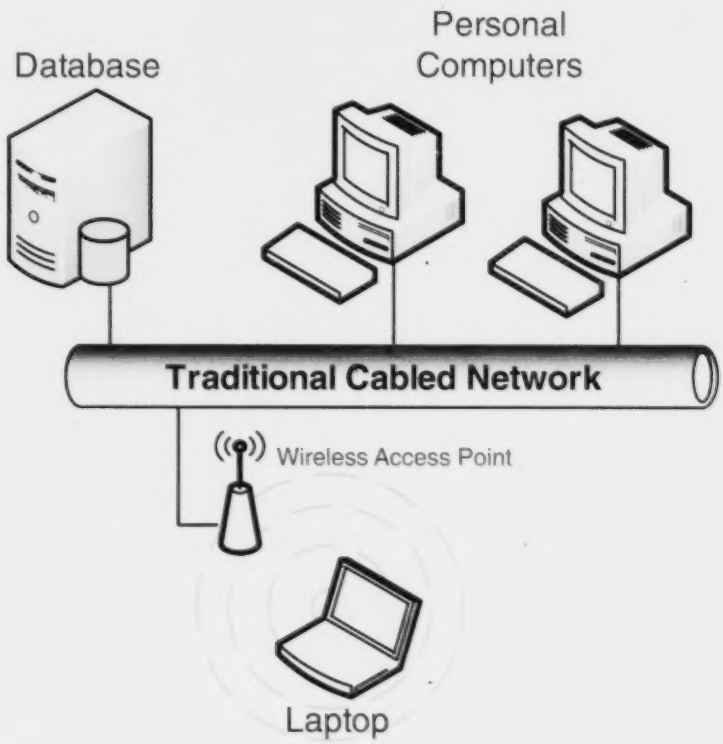
Wireless network environments are enabled in two common ways:

- In the most common way, one or more wireless access points are connected in an infrastructure mode network (Exhibit 1).
- In the second way—in what is called an ad hoc wireless network—two or more computers (such as laptops) are

connected wirelessly and transfer information back and forth. In an ad hoc network, there is no base station and every computer can talk directly to the other computers because their access cards are all set to the same channel and same network address (Exhibit 2). When one machine wants to "talk" to another, it transmits the data on the appropriate channel. In this situation, every computer "hears" the transmission, but only the receiving machine pays any real attention.

Exhibit 1:

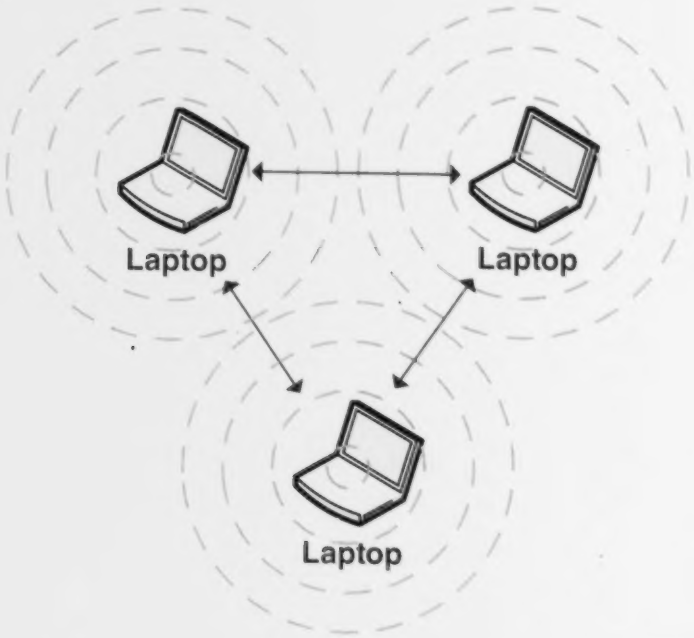
Example of wireless infrastructure mode networking



Source: Compiled by the Office of the Auditor General of British Columbia

Exhibit 2:

Example of wireless ad hoc networking



Source: Compiled by the Office of the Auditor General of British Columbia

Not properly managed, wireless computing poses significant information security risks to any person or organization using it

Many offices use wireless networks as an extension of their existing wired networks. The main advantage of wireless technology is its flexibility. It helps organizations extend their corporate network and allow for movement within the office or premises much more quickly, efficiently and often more cheaply than if they adopted a wired solution. In many businesses—and particularly in educational institutions—being able to roam the premises and remain in constant contact with the Internet and other network resources is essential to making effective use of users' time. It also helps support a "less paper" working environment.

The significant benefits of wireless computing, however, come with a price.

Because wireless devices broadcast their transmissions to anyone within range and who has the correct equipment, information meant for access by one party only is at risk of being received and read by many others. The result can be highly damaging if those individuals intercepting data have malicious intent, or even if they are just curious.

Thus, if wireless networks are not carefully designed and secured with proper device authentication and management controls, and if strong data encryption during transmission is lacking, even relatively small segments of a wireless network can put the entire network at high security risk. For example, if wireless network access points are not properly installed, signal leakage outside of the physical premises can propagate. These signals might then be picked up by individuals using wireless scanning equipment or a wireless-enabled device such as laptop, cell phone or PDA (personal digital assistant) in lobbies, cars or nearby parking lots (Exhibit 3). Risks increase in multi-tenant buildings, where only a single wall, ceiling or floor may stand between a wireless access point and scanning equipment.

In situations where access points are broadcasting data with weak or no encryption, all the data received and transmitted through them could be intercepted and copied. Of greatest concern are "keys to the kingdom" data—that is, sensitive information such as user-ids and passwords which, if picked up, could put an entire network under significant security threat. Ad hoc networking is particularly vulnerable, affording little authentication management and security. Base station operators with malicious intent can connect directly to authorized users and thus gain access to the enterprise network.

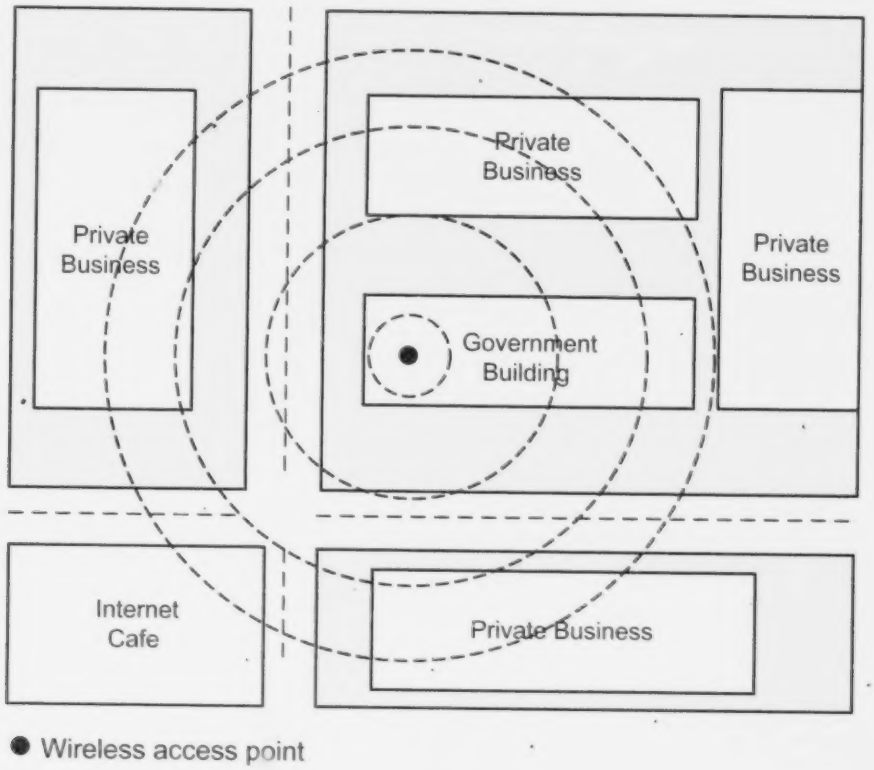
Whichever way a wireless network is enabled—infrastructure mode or ad hoc—an organization may be under surveillance yet never be aware of what is happening until a breach is realized.

As new and stronger data encryption methods are developed for wireless data transmission, so are new ways of breaking those encryption systems. Computer scientists in Japan, for example, recently developed a way to break the common Wi-Fi encryption (WPA- Wi-Fi Protected Access, which was considered acceptable in

securing wireless technology) in about one minute. Once a hacker can read encrypted traffic sent between computers and certain types of routers, he or she may launch any number of attacks on the network (see sidebar). Threats such as this make it important for organizations to use the strongest encryption system available to them.

Exhibit 3:

In a downtown area, considerable signal leakage can occur from a wireless access point



Source: Compiled by the Office of the Auditor General of British Columbia

Wireless network attacks can be carried out in several ways

The most common way that wireless installations are attacked is by individuals who, equipped with a specially enabled laptop computer fitted with an external antenna, drives or walks around buildings to find where signal leakage is occurring from wireless access points. The transmission information captured reveals whether the wireless access point is using encryption or not.

After an individual finds out which wireless access points have no or weak encryption, the way is open – if he or she is so inclined – to carry out a variety of attacks, as summarized in the table below. Unfortunately, the Internet makes available free software that can assist hackers in receiving and processing wireless signal scans, as well as in deciphering some types of encryption. Strong encryption is therefore a very important element in protecting any wireless network environment.

Common methods of attacking wireless networks

Type	Method	Example
Passive attacks	Eavesdropping	Attacker reads and captures message content from the air waves at particular sites.
	Traffic analysis	Attacker monitors data transmissions to look for patterns.
Active attacks	Masquerade	Attacker impersonates an authorized user and his or her privileges to gain access to systems and data.
	Replay (or "man-in-the-middle")	Attacker actively eavesdrops after independently connecting with two victims and then relays messages between them, making them believe they are talking directly to each other over a private connection. In fact, the attacker controls the entire conversation.
	Message modification	Attacker alters a legitimate message by deleting or modifying it.
	Denial-of-service	Attacker floods a wireless network with excess radio signals to prevent authorized users from accessing it.

Attacks on wireless computing networks from outsiders are not the only problem. Sometimes users will secretly attach their own wireless access points to a network without the knowledge of those who administer the security of the network. These unauthorized, or rogue, wireless access points pose a significant risk, since they may be installed inside the firewall set up to protect an organization's information assets from other types of external attacks.

Network-monitoring software is available that may detect rogue wireless access points. Using it, however, is often less effective than just performing onsite wireless scans to find the physical locations of wireless access points and determines whether they should be connected to the regular wired network.

What we looked at

Audit purpose and scope

For an organization to protect the confidentiality, integrity and availability of information exchanged in its wireless local area network (WLAN), it is essential that the organization:

- establish adequate policies, procedures, guidelines and standards for managing WLANs;
- protect against attacks on wireless data transmissions by using the strongest security settings available for computing devices; and
- monitor all network activities to detect unauthorized activities.

The purpose of our audit was therefore to assess whether the government and two educational institutions in British Columbia:

- have put into place adequate policies, standards, and procedures for managing their wireless networks;
- are securing their wireless networks through the proper configuration of wireless devices and implementation of control procedures; and
- are adequately monitoring wireless activities.

We conducted detailed wireless security assessments at five ministries and two post-secondary institutions, Simon Fraser University (SFU) and British Columbia Institute of Technology (BCIT). The five ministries were: Attorney General; Children and Family Development; Citizens' Services (which was with Ministry of Labour at the time of our audit); Health; and Labour.

We selected these ministries because some of their program activities include collecting sensitive information, thus making a secure and robust wireless network absolutely necessary. We performed internal and external scanning of wireless access point signals at a sample of those ministries' offices in cities across the province.

We selected SFU and BCIT because wireless technology is widely deployed within both post-secondary institutions. We performed an internal and external scanning of wireless access point signals at a sample of buildings on campuses of each institution.

The audit was carried out between July and September 2009, during which time we collected more than 7,000 signals from sites we visited:

- government offices: 3,570
- SFU: 1,518
- BCIT: 2,003

Our approach

We conducted the audit in accordance with the assurance standards recommended by the Canadian Institute of Chartered Accountants. Accordingly we included tests and other procedures we considered necessary to obtain sufficient and appropriate evidence to support our conclusions.

Traditional audit techniques were used in assessing non-IT/IM (information technology and management) areas, combined with walking around and inside office buildings to detect any rogue wireless access devices. The traditional audit techniques included reviewing:

- the IT plans for each organization, along with the documented process for approving wireless device implementation; and
- the documentation of activity logging and reporting within each organization to determine how it monitors and reports its compliance with wireless security policies.

We used the so-called "war-walking" technique in scanning wireless access points, moving around inside and outside of selected buildings. The scanning requires special software and hardware to detect and capture wireless access points data traffic. Captured data was analyzed to determine whether the organization's devices had proper security settings in accordance with policies and standards for securing wireless networking.

This analysis also provided a good indication whether they were emitted from wireless access points inside the building. Information gathered from war-walking also indicated how well the devices are physically protected. Our legal counsel confirmed that this method of collecting data traffic did not violate provincial privacy law. In all cases, the internal scanning of buildings was carried out unannounced and we obtained proper authorization at the site before entering the buildings.

We also assessed whether each organization had established clear business requirements for using wireless technologies and whether a risk assessment is regularly completed for implementing them.

- Our audit program and assessment criteria were based on the best practice guide *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*, published by the *National Institute of Standards and Technology*.
- We also used references from publications of the Information Systems Audit and Control Association (ISACA) in developing our audit program and criteria.

Our Audit Criteria

A. Maintain effective management of wireless security

a) Establish and maintain adequate policies, procedures, guidelines and standards for WLANs
b) Assign responsibility for wireless security
c) Maintain documentation of wireless architecture
d) Formally approve wireless technology deployment
e) Maintain a current list of wireless approvals
f) Use secure methods to administer wireless devices

B. Secure wireless infrastructure

a) Securely configure wireless devices
b) Deploy updates and security patches
c) Encrypt wireless traffic
d) Implement additional controls to secure networks accessible by wireless devices
e) Implement physical security controls to limit unauthorized wireless activity

C. Monitor wireless security

a) Maintain an inventory of wireless devices on the network
b) Monitor wireless activity logs
c) Monitor for unauthorized wireless activities

Detailed Report

What we did not look at

All users must be authenticated once they are logged onto a network through wireless access points. We did not look at the back-end authentication process of users. As important as that aspect is, it involves the review of backbone network infrastructure, database and server security and integrity. We also did not review the IT network infrastructure designs for those organizations.

The devices used to log onto wireless network are mostly laptop computers. All such devices should have secured configurations such as disabling ad hoc networking capability and blue-tooth connectivity, as well as be installed with an up-to-date virus application and security patches. We did not examine the configuration of users' computing devices in this audit. In our view, the front line of defense should be at the wireless access devices. Furthermore, given that users' computing devices vary in specification and operating systems, we did not feel it was possible to conduct such a review in an effective way.

Finally, we did not include in our audit a review of hand-held devices such as Blackberries and cell phones because they involve a different wireless technology than the "Wi-Fi" technology used by laptops.

We recognize that several of these areas warrant separate examination, and we plan on reviewing many of them in future.

What we found

Government

Shared Services BC, operating under the guidance of the Government Chief Information Officer (GCIO) in British Columbia (described below), provides wireless installation, maintenance and support for the provincial government and of broad public sector. Currently, the number of wireless device installations managed by Shared Services BC is limited. Most of those that do exist are located in the Greater Victoria area.

Wireless technology has not been adopted government-wide in British Columbia. The decision to adopt wireless technology is with the ministries' management, as long as they believe that there is

Architecture and Standards Review Board

The Government Chief Information Officer is Chair of the Chief Information Officer Council, which is made up of ministry Chief Information Officers. The Chief Information Officer Council discusses government IM/IT strategic issues, including any upcoming policies or systems. It also proposes architecture and standards, as well as changes to those.

In turn, the Architecture and Standards Review Board is responsible for reviewing and the council's proposals and making recommendations for approval to the OCIO. Approved policies and systems are incorporated into the GCIO's *IM/IT Architecture and Standards Manual*, which provides government-wide IM/IT guidance.

a need and budget allows. All requests to install wireless devices must be through Shared Services BC and ministries are not allowed to install wireless devices themselves.

The GCIO is the senior executive who establishes policies and strategies for the province's government IM/IT areas—including wireless technologies. As head of the Office of the Chief Information Officer (OCIO), the GCIO has a leadership role in re-engineering government's business processes and the underpinning IT infrastructures to increase the productive, efficient and valuable use of information (see sidebar).

It is the GCIO's *IM/IT Architecture and Standards Manual* that provides government-wide IM/IT guidance. The manual, implemented in February 2009, includes policies on wireless IT infrastructure, security and usage.

Overall Conclusion

The security around government's wireless infrastructure is generally adequate, but the process of monitoring wireless networking activities must be strengthened to ensure ministries are in compliance with policies and procedures to safeguard wireless transmissions.

Policies, procedures and other guidance related to wireless networking are adequate, but processes for ensuring ministry compliance are not

We found that government's current polices, standards and procedures are adequate to provide ministries and other government entities with guidance in deploying, monitoring and maintaining wireless infrastructure. However, processes for ensuring ministry compliance with that guidance are not as strong as they should be to ensure no unauthorized wireless access devices are connected to the government network.

We also found the job descriptions of key IT personnel at Shared Services BC to be well written, clear and current. The one exception was the job description of the Director of IT Security Operations, which has not been updated since November 2006.

Recommendations

We recommend that, to support the government's IM/IT policies relating to wireless network security, the government establishes adequate procedures to ensure ministry compliance with the policies as established by the OCIO.

We recommend that Shared Services BC regularly update the job descriptions of all key IT personnel to ensure the roles and responsibilities are clearly delineated.

Detection of unauthorized connectivity to government networking needs improvement

While Shared Services BC is charged with managing government's wireless technology and infrastructure, the decision for establishing wireless connectivity rests with each ministry. That decision is rarely based on a business case, as the cost of adding wireless devices is minimal. Thus, Shared Services BC will configure and install wireless devices whenever an approved request is received from the ministry.

Because those wireless devices currently need to be setup individually and not linked to a central control box, the ability to monitor them remotely is limited. As a result, unauthorized wireless computing devices connected to the government's network cannot be detected in real time.

Recommendation

We recommend that the government develop a network access control solution for monitoring and detecting, on a real time basis, unauthorized computing devices—particularly wireless—connected to the government network, including devices that are not configured properly.

Monitoring unauthorized wireless devices needs improvement

In general, we found that the government has an adequate process in place to ensure that wireless access points and devices are configured appropriately. The requirement for user authentication before being allowed access to the government network infrastructure is also adequate. However, because the government lacks the ability to perform real-time detection of unauthorized wireless access devices or computing devices connected to the government network, there is risk of inappropriately configured wireless devices being installed without ready detection.

Currently the government is relying on its network system authentication or specific application authentication procedures to restrict access to the government network and applications to authorized users. The authentication process is outside the scope of this audit, but we have no reason to believe it is not adequate to prevent unauthorized users from accessing the government network. Nevertheless, we think that network security would be strengthened with the frontline defence of detecting unauthorized devices on a real-time basis.

During our war-walking scans at the offices of the five ministries we audited, we detected 3,570 signals. Of those, we determined that 1,946 signals were deployed within government office premises but were not from devices managed by Shared Services BC or a ministry. Through a detailed analysis, we concluded that 141 of the signals were questionable—and 52 we determined, after consulting Shared Services BC, were highly suspicious. In addition, they were either configured without encryption, or using a weak encryption protocol, and none had been installed by Shared Services BC.

We also detected many signals that had strong encryption. We did not provide them to Shared Services BC for follow-up because we consider them to be lower risk than the others. These signals could have been coming from either non-authorized or authorized devices managed by Shared Services BC.

Recommendation

We recommend that Shared Services BC implement mechanisms and procedures to scan and confirm that only properly configured and authorized wireless access devices are installed when connecting to the government network infrastructure.

Monitoring wireless activities needs improvement

Although Shared Services BC has adequate procedures for logging in requests from ministries for changes to or additions of wireless access devices, these procedures are not linked with an inventory system of authorized wireless access devices.

We also found that although event logs of network activities exist, these logs are not specific to wireless network activities because all of the devices are autonomous. As a result, the government has no effective means of monitoring wireless network activities. The above recommendation with regards to the implementation of

mechanisms and procedures to scan and confirm that only properly configured and authorized wireless access devices are installed can help to mitigate this control deficiency.

Recommendation

We recommend that for monitoring purposes, Shared Services BC develop a process for establishing and updating an inventory list of authorized wireless access devices, and that the list is periodically verified.

Simon Fraser University (SFU)

Simon Fraser University has an extensive framework for deploying a wireless infrastructure and coverage for all of its campuses. The main campus is in Burnaby. The others are Harbour Centre (Vancouver), Centre for Dialogue (Vancouver), Segal Graduate School (Vancouver) and Surrey Campus.

More than 30,000 students and about 3,000 staff, employees and guests can access the university's wireless network.

Responsibility for the deployment of wireless networks at SFU is with the Network Services Department. The Associate Director of IT Services Division approves requests submitted by departments for wireless coverage. The Network Services Department is also responsible for monitoring activities in the wireless network and maintaining the infrastructure. Security of the wireless infrastructure is the responsibility of the department's Network Engineering group.

Overall Conclusion

Simon Fraser University's wireless network security is generally adequate, but improvements are needed in areas such as: enhancing policies and standards in wireless networking; strengthening the governance structure of IT division, the management and monitoring of wireless operating activities, as well as the roles and responsibilities of staff who are charged with the responsibilities of overseeing the IT security.

Stronger IT governance is needed, wireless networking policies need strengthening, and formal user acceptance of appropriate use of technology be made mandatory

Simon Fraser University has policies to guide deployment and management of its wireless infrastructure for all campuses. However, we found three areas of weakness:

- No formal IT committee exists to oversee the university's IT strategic direction, policies and operations. Responsibility for the university's IT strategic plan and operations rests with the Office of the Chief Information Officer (CIO), reporting to the Vice-President, Finance and Administration and to the Associate Vice-President, Academic. In our view, while this approach may be adequate for meeting the day-to-day IT requirements of staff and faculty, it does not provide strong governance for managing the short- and long-term IT needs of SFU. Such governance is needed to ensure that adequate resources are allocated to support a robust, secure university IT network.
- The university lacks detailed standards for ensuring the security of its wireless infrastructure. The Information Security Policy addresses some security aspects, but it is not comprehensive enough to lay out specific security standards. In keeping with best practices, entities should have formal, written standards and related procedures that address such security matters as configuration requirements for all computing wireless devices and authentication procedures.
- Although SFU has a "Fair Use of Information and Communications Technology" policy, there is no policy acceptance by users for appropriate use of IT resources when logged onto the university network. Best practice suggests users acceptance of the established policy when logging onto the network. This practice will ensure users are aware of the policy and also provide the university the right to repudiate their access privileges if they violate the established policy.

Recommendations

We recommend that the university:

- ***establish a formal IT committee with a strong mandate to oversee IT strategic direction, IT needs of the university community and, most importantly, the protection of the university's IT network;***

- ***ensure that the Information Security Policy is supported with detailed wireless security standards and procedures to guide the implementation and maintenance of a robust wireless security network; and***
- ***establish policy and procedures to ensure that users are formally and regularly asked online to accept the policy for appropriate use of communication technology (including wireless) provided by the university.***

Separation of duties within IT Services Division needs strengthening, as does the management and monitoring of wireless operating activities

The Network Engineering group is responsible for ensuring the security of the university's IT network, including wireless. That job has been assigned to a staff member in Security Services who has network administrative duties. Our review of the organization chart showed that this individual reports to the Director, Network Services.

We do not believe that this reporting relationship is strong enough to ensure that incidents of IT security breaches receive timely and adequate resolution. In keeping with best practices, the university would require a dedicated IT Security Officer who reports directly to a senior executive such as the President of the university or the Chair of an IT committee. The key responsibilities of this individual should be to: oversee network security; investigate security breaches; manage the development and implementation of a global security policy, standards, guidelines and procedures; and work with outside consultants, as appropriate, to conduct independent security audits.

We found several other weak areas in security as well:

- The university gives employees two ways of connecting to the wireless network: through SFUNET (which is non-secure) and through SFUNET (secure). We found no polices or procedures that make it mandatory for employees to only use the secured wireless access when they log on to the SFU wireless network.

We were told that SFU conducts war-walking scans twice a year, inside and outside buildings, around its campuses. We did not assess the methodology used in these exercises and therefore cannot comment on their effectiveness. However, of the more than 1,500 internal wireless signals we detected during our war-walking around SFU's campuses and selected buildings, we found that:

- 17 were not on the list the university gave us and were broadcasting using an SFU ID as a non-secured connection;
- 10 were not on the list the university gave us and were broadcasting using an SFU ID as a secured connection; and
- 4 were on the list the university gave us but were broadcasting using a non-SFU ID.

We believe that the Network Services Department should investigate these wireless signals to determine the reasons why they were not set up in accordance with the university's device security requirements.

- Our scanned results also revealed 43 instances of ad hoc and peer-to-peer networking. We found that the university has no effective policies and practices requiring ad hoc and peer-to-peer networking to be disabled.
- The university does not require users to change passwords after a fixed time interval. We believe that this is not a good practice in enhancing strong network security.

Recommendations

We recommend that the university:

- ***establish an IT Security Officer position that has exclusive duties and responsibilities relating to IT security and is accountable to independent senior management;***
- ***conduct reviews to limit the use of ad hoc and peer-to-peer networking;***
- ***enforce periodic password changes; and***
- ***require staff with high-level access rights to systems, applications and data to only access system resources using secured wireless methods.***

Monitoring wireless activities need to be strengthened

The university has a diverse community and a complex business environment. Given that its key businesses are in research and education, its IT service model is designed to provide both researchers and students with as much flexibility or freedom as possible to carry out their research and learning activities. This independence means that the acquisition, configuration, use and disposal of computing equipment are not centralized responsibilities of the Network Services Department.

University management knows the risks posed by this situation and has determined that the biggest threat to SFU's data security is from within its own community. To compensate for this weakness, IT management has designed and implemented a multi-layer security framework for protecting sensitive data—one with strong controls over user access rights and authentication at the system and application levels.

The effectiveness of this security architecture is not part of the scope of this audit, but we have no reason to believe it is not working effectively.

The request for wireless access device installation is reviewed and approved by the Associate Director, Network Services, before the wireless device is configured and deployed. For those wireless access devices that were purchased and installed by Network Services, there is minimal threat to network security, as they are centrally controlled and configured and they cannot be configured to work as a normal wireless access point. Management functions of the wireless infrastructure are mostly software driven, such as activation and deactivation of wireless access points, performance monitoring and monitoring of network activities. The software is capable of generating performance results and logging most activities in the network.

Logs of network activities are stored at various network centres. The logs are continuously analyzed by Network Services for anomalous activities. When anomalies are detected, network personnel are notified so appropriate action can be taken. All system administrators have "read only" access to the logs, but log review and maintenance is the responsibility of the Network and System Administrator. The network management software is capable

of generating a variety of reports from the logs, such as users logged in, traffic through the network, access points' status and unauthorized activities.

We noted that although the Network and System Administrator reviews the logs, documentation of review activities is poor, leaving no audit trail showing how often the review is done, what type of reports are reviewed, and what actions have been taken, if any.

Recommendation

We recommend that the university, in monitoring wireless networking activities, ensure that log reviews are fully documented and include such information as the type of reports reviewed, the date of the review, and what action has taken place.

British Columbia Institute of Technology (BCIT)

An extensive framework for deploying the wireless infrastructure exists at BCIT. The main campus is in Burnaby, with other campuses located in downtown Vancouver, Richmond and North Vancouver. All of the campuses have access to the BCIT wireless network. Some of BCIT's satellite offices in other locations—Surrey, North Vancouver, Langley, Burnaby, Kelowna, Coquitlam and Maple Ridge—also have wireless access.

In all, more than 50,000 students (full-time and part-time) and about 2,500 staff, employees and guests can access the college's wireless network.

The Technology Enabled Knowledge (TEK) plan is the key driving force in deployment of the wireless infrastructure at BCIT. TEK is a five-year, multi-million dollar plan to enhance teaching and learning at BCIT through the strategic use of technology. The TEK educational vision is based on providing students with the opportunity to learn new ways to communicate, participate and succeed in their communities and workplaces. Through the TEK initiative, advanced communication, teaching and learning approaches and devices are being placed in the hands of BCIT students, faculty, industry partners and administrators.

Overall Conclusion

Wireless network security at BCIT is generally adequate, but improvement is needed in areas such as: enhancing policies and standards in wireless networking; strengthening the management and monitoring of wireless operating activities as well as clearly defining the roles and responsibilities of staff within the IT division.

Wireless networking policies need strengthening

While BCIT's deployment of its wireless infrastructure is extensive, the college lacks adequately detailed wireless networking standards and procedures to support its policies for running a robust wireless environment.

The existing Information Security Policy briefly describes most parts of the IT infrastructure and touches on most security aspects, but it does not extend to the wireless infrastructure in detail. For example, in keeping with best practices, BCIT should have a written policy, along with related standards and procedures to address wireless network infrastructure, configuration, and deployment.

Recommendation

We recommend that BCIT ensure its policies address wireless network infrastructure in detail, and that the policies be supported by detailed wireless networking standards and specific procedures and guidelines for managing wireless network resources.

Management of Wireless network activities needs to be strengthened

At BCIT, all expansions of the wireless infrastructure to increase its coverage take direction from the TEK initiative. The change management procedures for this are adequate and are followed during network deployment.

Both the college's Acceptable Use of IT Policy and IT Security Policy are guiding BCIT in implementing and using its IT infrastructure. However, the policies do not address the disabling of ad hoc or peer-to-peer networking, password changes, or the review and retention of log files.

Recommendation

We recommend that BCIT's management review its policies to ensure that those relating to ad hoc and peer-to-peer networking, the enforcement of password security, and retention of activity logs generated by wireless systems follow recognized best practices.

During our war-walking scans at selected buildings of the Burnaby, downtown Vancouver, Richmond and North Vancouver campuses, we collected more than 2,000 wireless access point signals. Our analysis revealed 334 instances of signals having no encryption. After discussions with the college's IT Services group, we determined that of the 334 non-encrypted signals:

- 274 belonged to BCIT because, as the IT network team confirmed, BCIT is using unsecured connectivity to reduce administrative overhead costs;
- 2 were from access points configured close to BCIT configuration patterns at the North Vancouver campus; and
- the remaining 58 included some having names or patterns close to those of BCIT's infrastructure.

As well, we noted instances of data traffic from access points and servers in clear text. Although they were using unsecured connectivity, we were informed that all sensitive applications are using a secured communication channel to provide encryption and securing identification of servers. We believe this is adequate in preventing "listening-in" by others.

We found that users of the BCIT wireless network are properly authenticated, being required to input their credentials before being allowed to access the wireless infrastructure. Appropriate physical security mechanisms over wireless devices are also in place. Those devices are either installed near or above the ceiling to prevent the devices being damaged or stolen. However, we found no requirement by BCIT for staff and administrators to log on to the network using secured wireless access only. This weakness poses a potential threat to the network's security, especially if staff with high-level access rights to systems do not always log on through secured wireless methods.

Recommendation

We recommend that management require, in policy, staff with higher level access rights to systems, applications and data to only log on using secured wireless methods.

Monitoring wireless activities is adequate

The network team that forms part of the IT Services group at BCIT is responsible for maintaining the inventory of wireless devices using the college's wireless network. Most of the team's monitoring activities are software driven. Currently, network activity logs are monitored manually by reviewing the "event-driven" log. However, we found that the log review process is carried out independently from activities to detect wireless intrusions.

Having already recognized this problem, BCIT is now working to integrate the activities with its Security Information Management Solution application.

Roles and responsibilities of IT staff needs to be defined clearly

We observed the college's IT staff who are charged with looking after BCIT's wireless network were carrying out incompatible duties. They were being allowed, for example, not only to propose changes to the network, but then to make and sign off on those changes. We also noted that the roles and responsibilities of these same IT staff are not clearly defined for each job position.

While we recognize that the job descriptions relate to a function and are approved through the Collective Bargaining Agreement, we think it is important that each job description for key IT staff be supported by clearly defined roles and responsibilities to ensure incompatible duties are not assigned.

Recommendation

We recommend that job positions in IT network operations be supported by clearly defined responsibilities to ensure incompatible duties are not assigned to one individual. If segregation of duties is not possible or feasible because of resourcing limitations, we recommend that there be closer management oversight of the activities carried out by those in IT network operations.

Appendices

Appendix A: Glossary

Commonly seen and used in wireless technology

Access Point

An electronic device that logically connects other wireless computing device, such as laptops, PDA, Blackberry, etc. into a network, which is typically an organization's enterprise wired network. *(Source: Guide to Securing Legacy IEEE 802.11 Wireless Networks – National Institute of Standards and Technology)*

Ad Hoc Network

A wireless network that dynamically connects wireless client devices to each other without the use of an infrastructure device, such as an access point or a base station. *(Source: Guide to Securing Legacy IEEE 802.11 Wireless Networks – National Institute of Standards and Technology)*

Configure

To set up or arrange settings in computing systems or programs in order to achieve a specific purpose. (e.g. level of control restriction) *(Source: Office of the Auditor General)*

Denial of Service (DoS) attack

An attack on a network that is designed to bring the network to its knees by flooding it with useless traffic. *(Source: www.webopedia.com)*

Firewall

A firewall is designed to prevent unauthorized access to or from a network. It can be hardware, software, or a combination of both. All messages entering or leaving the network through the firewall are examined and those that do not meet the specified security criteria are blocked. *(Source: www.webopedia.com)*

Flooding

Flooding is a Denial of Service (DoS) attack that is designed to bring a network or service down by flooding it with large amounts of traffic. *(Source: www.webopedia.com)*

Encryption

Encryption is the translation of data into a secret code and is an effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. *(Source: www.webopedia.com)*

IEEE 802.11

Abbreviation of Institute of Electrical and Electronics Engineers, pronounced I-triple-E. IEEE is an organization composed of engineers, scientists, and students. The IEEE is best known for developing standards for the computer and electronics industry. In particular, the IEEE 802 standards for local-area networks are widely followed. *(Source: www.webopedia.com)*

Appendix A: Glossary

IEEE 802.11 is a set of standards carrying out wireless local area network (WLAN) computer communication in the 2.4, 3.6 and 5 GHz frequency bands. They are created and maintained by the IEEE LAN/MAN Standards Committee (IEEE 802). *(Source: www.wikipedia.org)*

There are several specifications in the 802.11 family:

- **802.11** – Original IEEE Standard for wireless LANs (WLAN) at rates between 1 or 2 Mbps transmission in the 2.4 GHz band. (not widely implemented or deployed)
- **802.11a** – IEEE Standard for WLAN at rates up to 54-Mbps in the 5GHz band.
- **802.11b** - IEEE Standards for WLAN at rates up to 11 Mbps transmission in the 2.4 GHz band.
- **802.11g** – IEEE Standards for WLAN at rates up to 54-Mbps in the 2.4 GHz bands and is used for transmission over short distances.
- **802.11n** – 802.11n builds upon previous 802.11 standards. The additional transmitter and receiver antennas allow for increased data throughput through spatial multiplexing and increased range. The real speed would be up to 4-5 times faster than 802.11g.

(Source: www.webopedia.com)

Infrastructure Network

A wireless network that requires the use of an access point to facilitate communication between computing devices. *(Source: Guide to Securing Legacy IEEE 802.11 Wireless Networks- National Institute of Standards and Technology)*

Jamming

An attack in which a device is used to emit electromagnetic energy on a wireless network's frequency to make it unusable. *(Source: Guide to Securing Legacy IEEE 802.11 Wireless Networks – National Institute of Standards and Technology)*

Log file

A file that lists actions that have occurred within computer, network or application use. *(Source: www.webopedia.com)*

Man-in-the-middle attack

The man-in-the-middle attack (often abbreviated MITM), or bucket-brigade attack, or sometimes Janus attack, is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all messages going between the two victims and inject new ones, which is straightforward in many circumstances (for example, an attacker within reception range of an unencrypted Wi-Fi wireless access point, can insert himself as a man-in-the-middle). *(Source: http://en.wikipedia.org)*

Appendix A: Glossary

Media Access Control (MAC)

A unique ID that is assigned to a particular wireless network interface by the manufacturer. Sometimes refer to as BSSID (Basic Service Set Identifier) *(Source: Guide to Securing Legacy IEEE 802.11 Wireless Networks – National Institute of Standards and Technology)*

Patch

Instructions written in computer language that are inserted into a computer program or system designed to fix a known problem or security vulnerability. *(Source: Office of the Auditor General)*

Physical access controls

Restriction of access to computers or network equipment only to authorized personnel. For example—a locked door with entrance control device such as numeric keypad or biometric device. *(Source: Office of the Auditor General)*

Range

The maximum possible distance for communicating with a wireless network infrastructure or wireless client. *(Source: Guide to Securing Legacy IEEE 802.11 Wireless Networks – National Institute of Standards and Technology)*

Robust Security Network

A network:

- that does not break down easily or is not wholly affected by a single application failure;
- a system that either recovers quickly from or holds up well under exceptional circumstances;
- a system that is not wholly affected by a bug in one aspect of it; and
- a system that comes with a wide range of capabilities.

(Source: www.webopedia.com)

Rogue access point

A rogue access point is a wireless access point that has either been installed on a secure company network without explicit authorization from a local network administrator. *(Source: http://en.wikipedia.org)*

Router

A router is an electronic device used to connect two or more computers or other electronic devices to each other, and usually to the Internet, by wire or radio signals. This allows several computers to communicate with each other and to the Internet at the same time. If wires are used, each computer is connected by its own wire to the router. *(Source: http://en.wikipedia.org)*

Appendix A: Glossary

Server

In computing, a server is any combination of hardware or software designed to provide services to clients. *(Source: http://en.wikipedia.org)*

Service Set Identifier (SSID)

A name assigned to a WLAN that allows stations to distinguish one WLAN from another. *(Source: Guide to Securing Legacy IEEE 802.11 Wireless Networks – National Institute of Standards and Technology)*

Traffic

Information load over a network either through WLAN or wired network. *(Source: Office of the Auditor General)*

Virtual Private Network (VPN)

A VPN, or virtual private network, is a network that is constructed by using public wires to connect nodes. For example, there are a number of systems that enable you to create networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted or altered. *(Source: www.webopedia.com)*

Wired Equivalent Privacy (WEP)

A security protocol, specified in the IEEE 802.11 standard, that is designed to provide a WLAN with a level of security comparable to what is usually expected of a wired LAN. WEP is no longer a viable encryption mechanism due to known weaknesses. *(Source: Guide to Securing Legacy IEEE 802.11 Wireless Networks – National Institute of Standards and Technology)*

Wi-Fi

The name of a popular wireless networking technology that uses radio waves to provide wireless high-speed Internet and network connections. The Wi-Fi Alliance, the organization that owns the Wi-Fi (registered trademark) term specifically defines Wi-Fi as any "wireless local area network (WLAN) products that are based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards." A common misconception is that the term Wi-Fi is short for "wireless fidelity," however this is not the case. Wi-Fi is simply a trademarked term meaning IEEE 802.11x. *(Source: www.webopedia.com)*

Wireless Local Area Network (WLAN)

A group of wireless APs and associated infrastructure within a limited geographic area, such as building or building campus, that is capable of radio communications. WLANs are usually implemented as extensions of existing wired LANs to provide enhanced user mobility. *(Source: Guide to Securing Legacy IEEE 802.11 Wireless Networks – National Institute of Standards and Technology)*

Appendix B: Security Guidelines for Wireless Area Networks

Policies

- Understand and adhere to all applicable policies, standards and guidelines for wireless infrastructure security.
- In the absence of applicable or outdated policy and standards, create an appropriate security policy with supporting standards for wireless LAN infrastructure.
- The policy should address aspects such as purpose, responsibilities, enforcement, exceptions, and terms and definitions.
- Maintain policies, standards and guidelines to ensure they are current and relevant with wireless LAN technology developments and new threats.

Controls

Utilize the following minimum controls when attaching a wireless LAN infrastructure to the government network:

- Utilize all the controls as stipulated in the appropriate government information security policy.
- Control physical access to wireless LAN devices to prevent malicious activities such as resetting device to default factory setting.
- Check regularly for vendor security patches and upgrades and apply as needed.
- Have regular, independent security assessments performed to measure compliance and check for rogue or unauthorized wireless devices.
- Maintain a complete inventory of all wireless LAN devices.
- If the business requirement exists, provide for wireless LAN guest access to avoid rogue access points connecting to internal networks.

Awareness and Training

Users and administrators of the wireless LAN need to be educated in wireless network security:

- Ensure that users on the wireless LAN are trained in information security awareness and the risks associated with wireless technology.
- Administrators must track progress of the latest wireless LAN standards and security features.
- Administrators must vigilantly monitor for new wireless LAN threats and vulnerabilities.
- Ensure staff clears wireless LAN device configurations before disposing of equipment to prevent disclosure of network configuration, keys, passwords, etc.

Monitoring and Audit

- Enable logging on wireless LAN devices and review logs on a regular basis for security-related events.
- Establish programs to detect rogue access points (unapproved internal network connections and attempts to mimic official networks to capture confidential information).
- If your wireless LAN does not provide for automated rogue detection, establish a manual audit program.
- Establish procedures for reporting and responding to wireless LAN security incidents.

Source: PriceWaterhouseCoopers, LLP

Appendix C: Useful Tips for Accessing and Using Government Networks

All users accessing government networks

Regardless of the method used to connect to a government network, these minimum security measures should be followed:

- Ensure that a personal firewall is enabled on your computer (i.e., McAfee).
- Install proven anti-virus software.
- Ensure your anti-virus software is up-to-date with the latest virus definition files.
- Keep your Windows (or other Operating Systems) up-to-date with the latest security patches.
- Do not open email attachments from unknown senders.
- Avoid file sharing by disabling this feature on your computer.
- Make regular backups of critical data.

In addition to these basic security measures, other specific ones must also be followed, depending on your access method.

Wired networks (ADSL, cable, dial-up)

To connect securely, use the Workplace Technology Services (WTS) security infrastructure such as:

- Virtual Private Network (VPN) to connect securely over the internet.
- Desktop Terminal Services (DTS).
- HTTPS security enabled websites, which you can recognize by the https in the URL address.

Wireless computing

- Change the default admin password on the wireless router.
- Enable strong encryption, ideally using Wi-Fi Protected Access (WPA).
- Turn the wireless network off when you will not use it for prolonged periods.
- Do not put personally identifiable information, such as your name, in wireless device identifiers (known as SSIDs).

Appendix C: Useful Tips for Accessing and Using Government Networks

HOTSPOTS (airports, cyber-cafés)

- Avoid using hotspots if transmitting any confidential or sensitive information unless you are using VPN or HTTPS.
- If you do not know what VPN or HTTPS is, you should not be using hotspots to transmit sensitive data.
- Watch out for shoulder surfing (people may be watching over your shoulders to obtain sensitive information such as user IDs and passwords).
- Avoid using ad hoc (peer-to-peer) wireless.

If in doubt, contact your system administrator for advice or instructions.

Source: PriceWaterhouseCoopers, LLP